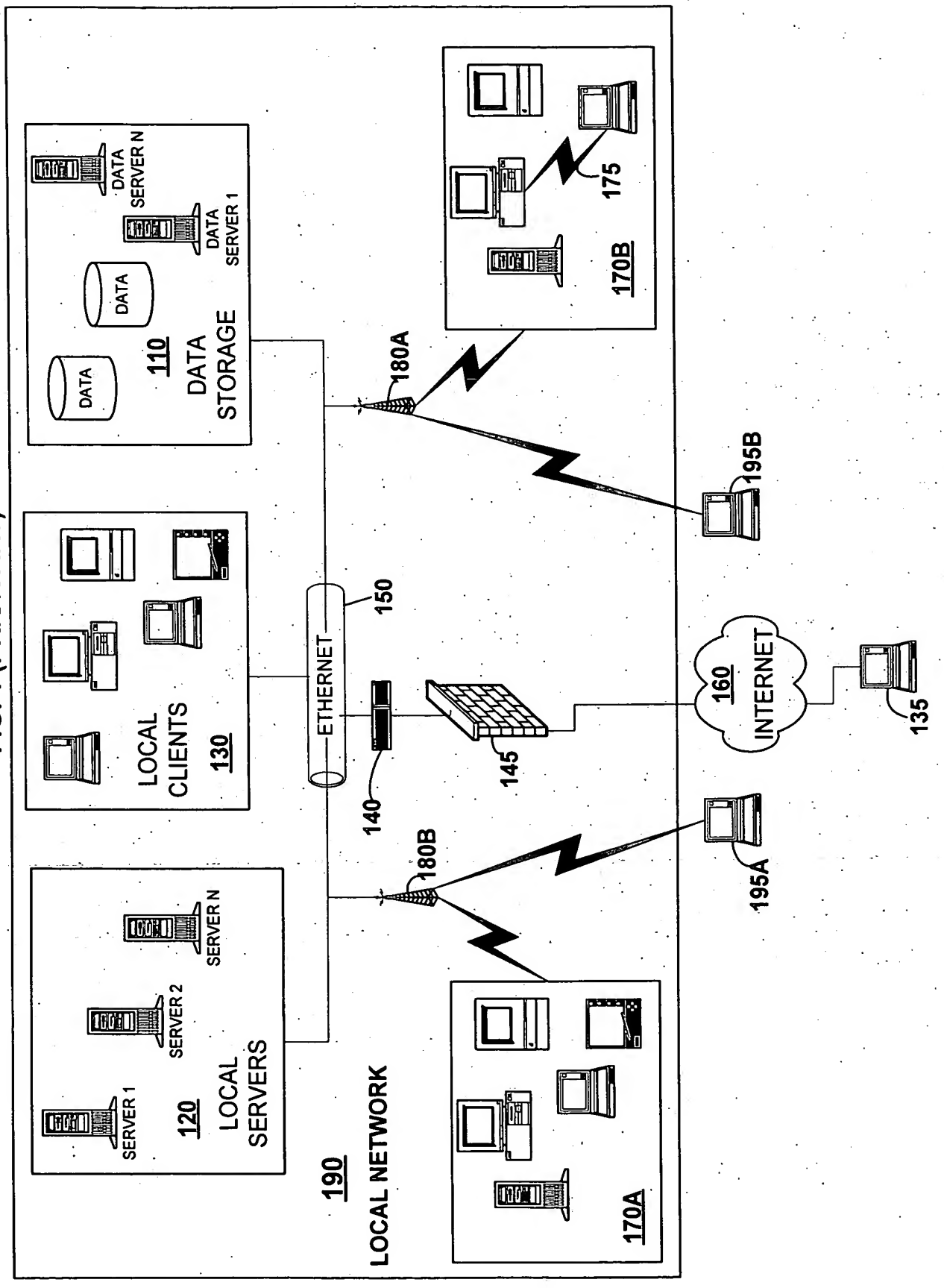


FIG. 1 (PRIOR ART)

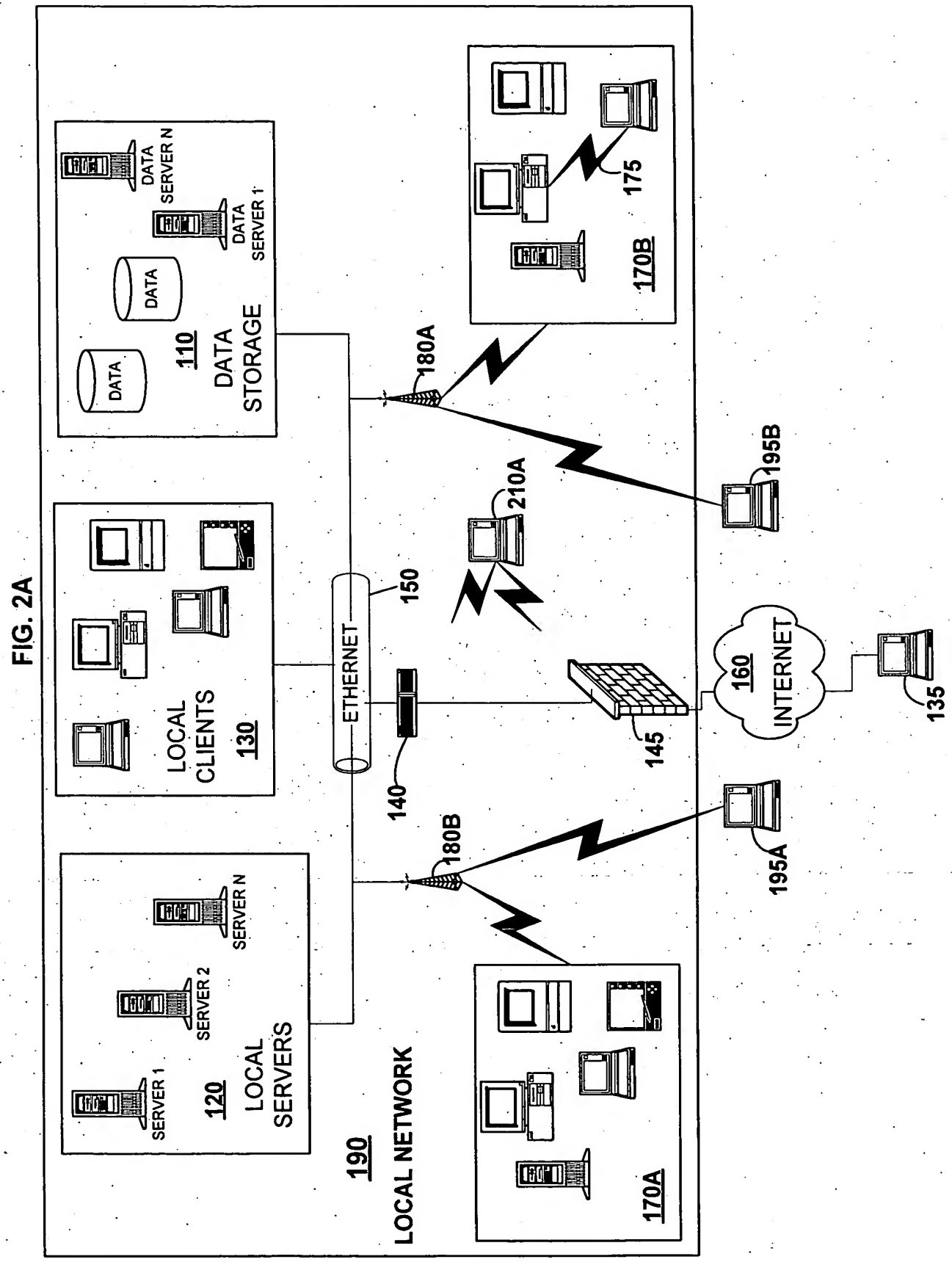

DATA SERVER N
DATA SERVER 1
DATA
DATA
110
DATA STORAGE
175
170B
180A
195B
210A
150
ETHERNET
LOCAL CLIENTS
130
140
145
160
INTERNET
135
180B
195A
SERVER N
SERVER 2
SERVER 1
120
LOCAL SERVERS
190
LOCAL NETWORK
170A

FIG. 2A

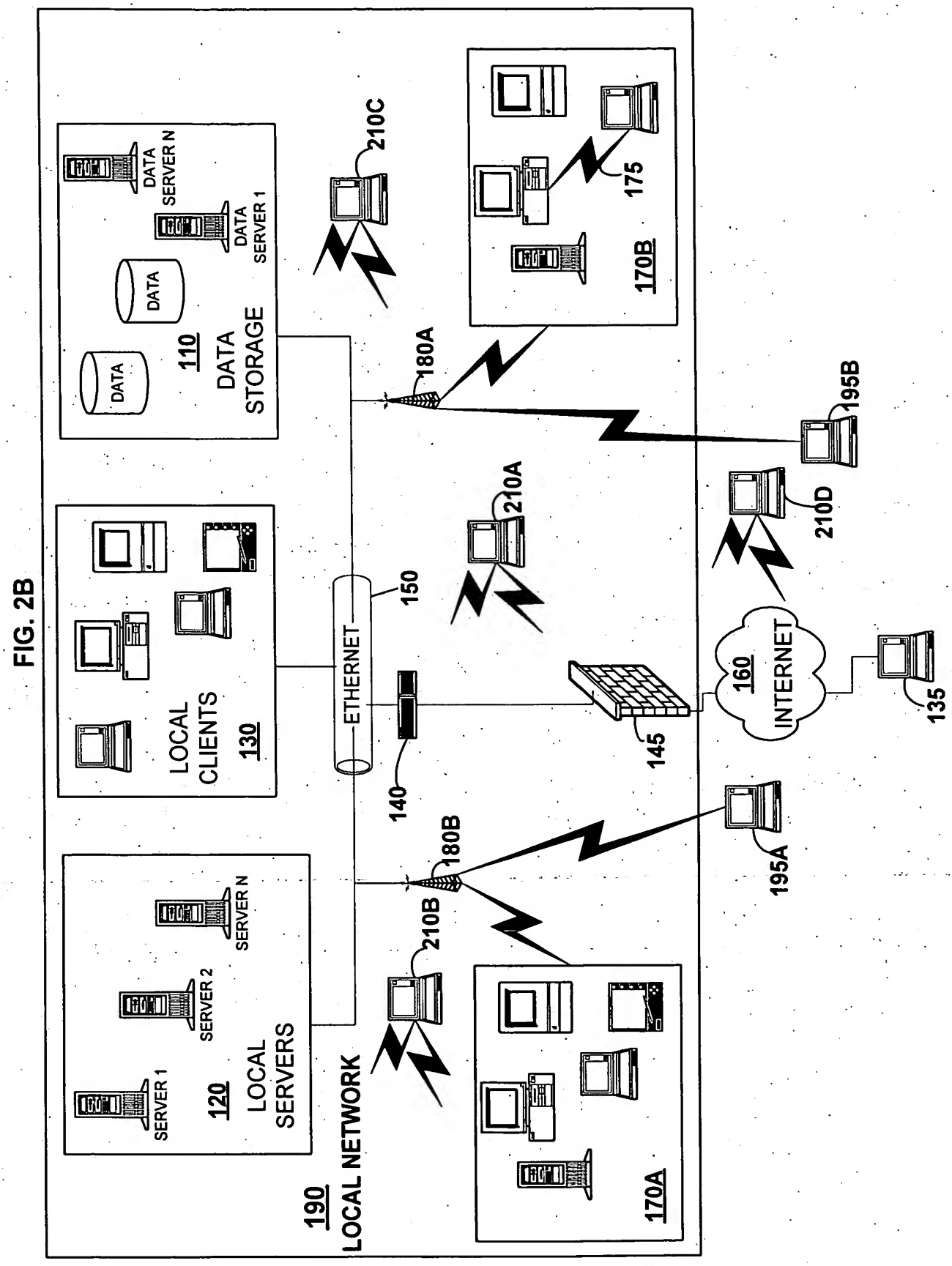

DATA SERVER N
DATA SERVER 1
DATA
DATA
110
DATA STORAGE
210C
175
170B
180A
195B
210A
210D
150
ETHERNET
LOCAL CLIENTS
130
160
INTERNET
135
145
140
180B
195A
SERVER N
SERVER 2
SERVER 1
120
LOCAL SERVERS
210B
170A
190
LOCAL NETWORK

FIG. 2B

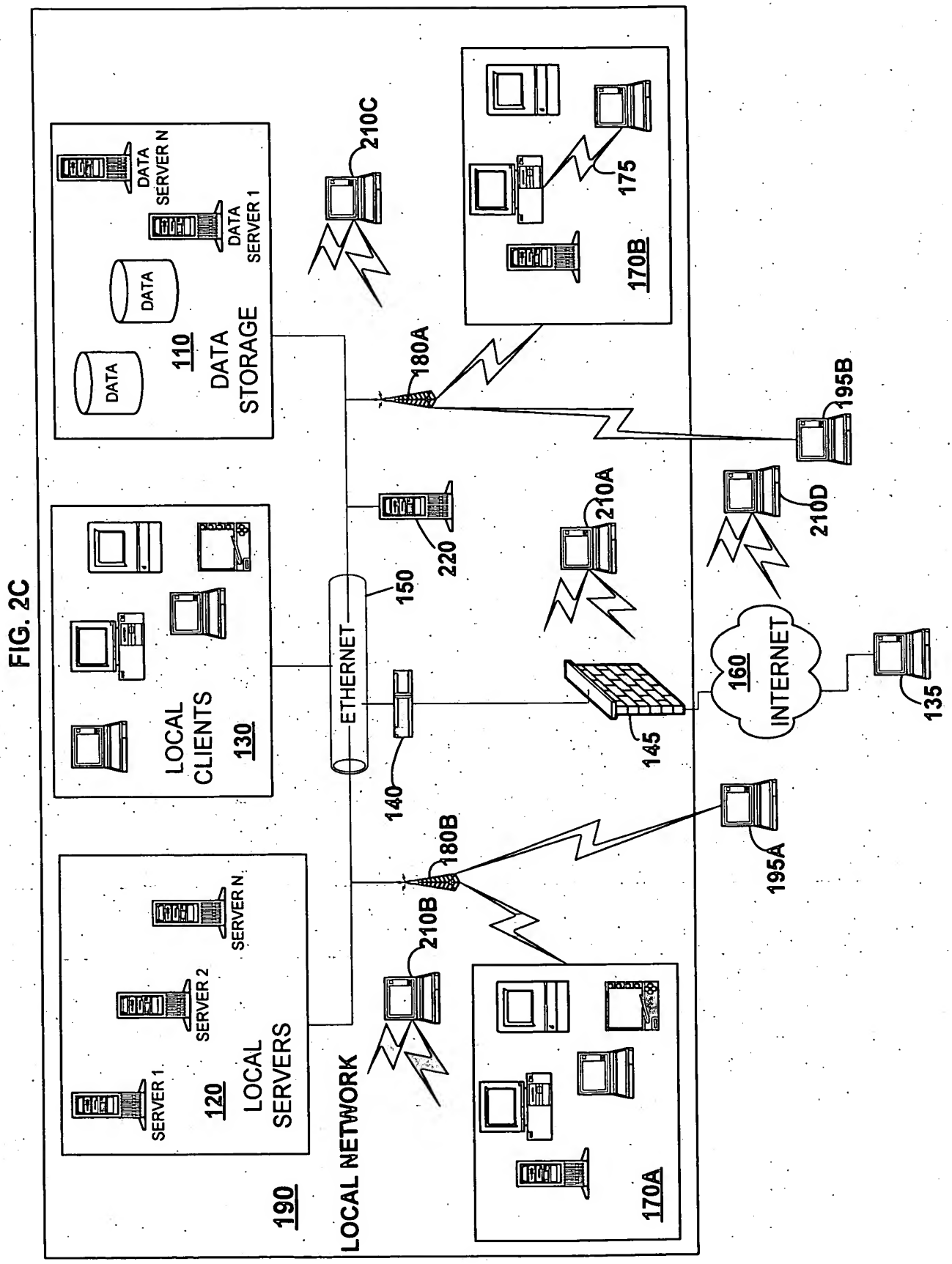

DATA SERVER N
DATA SERVER 1
DATA
DATA
110
DATA STORAGE
210C
175
170B
180A
195B
210D
210A
220
150
ETHERNET
LOCAL CLIENTS
130
140
145
160
INTERNET
135
195A
180B
210B
SERVER N
SERVER 2
SERVER 1
120
LOCAL SERVERS
190
LOCAL NETWORK
170A

FIG. 2C

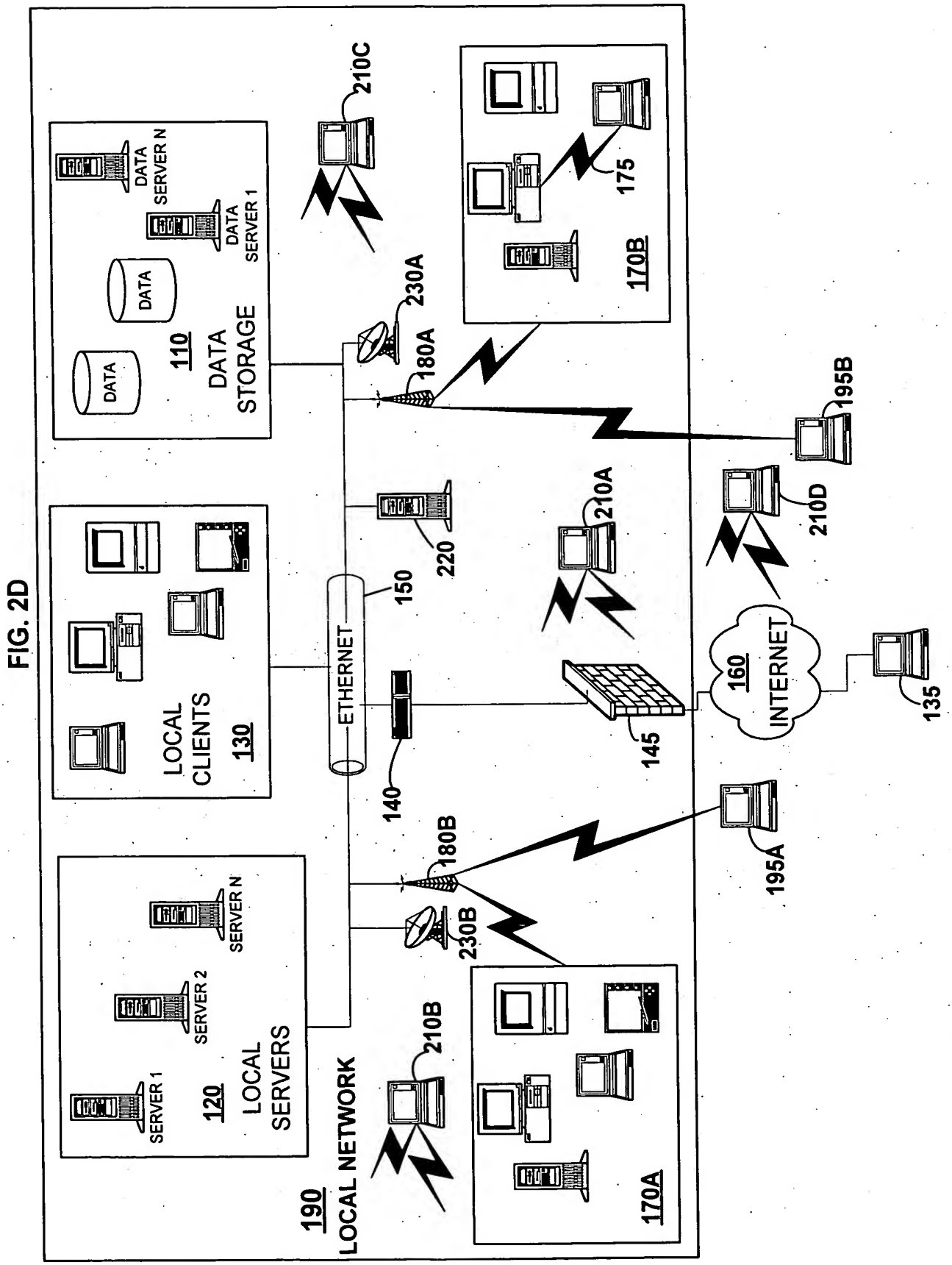

DATA SERVER N
DATA SERVER 1
DATA
DATA
110 DATA STORAGE
210C
175
170B
230A
180A
195B
210D
210A
220
150
ETHERNET
LOCAL CLIENTS 130
160 INTERNET
135
145
140
180B
195A
230B
SERVER N
SERVER 2
SERVER 1
120 LOCAL SERVERS
210B
170A
190 LOCAL NETWORK

FIG. 2D

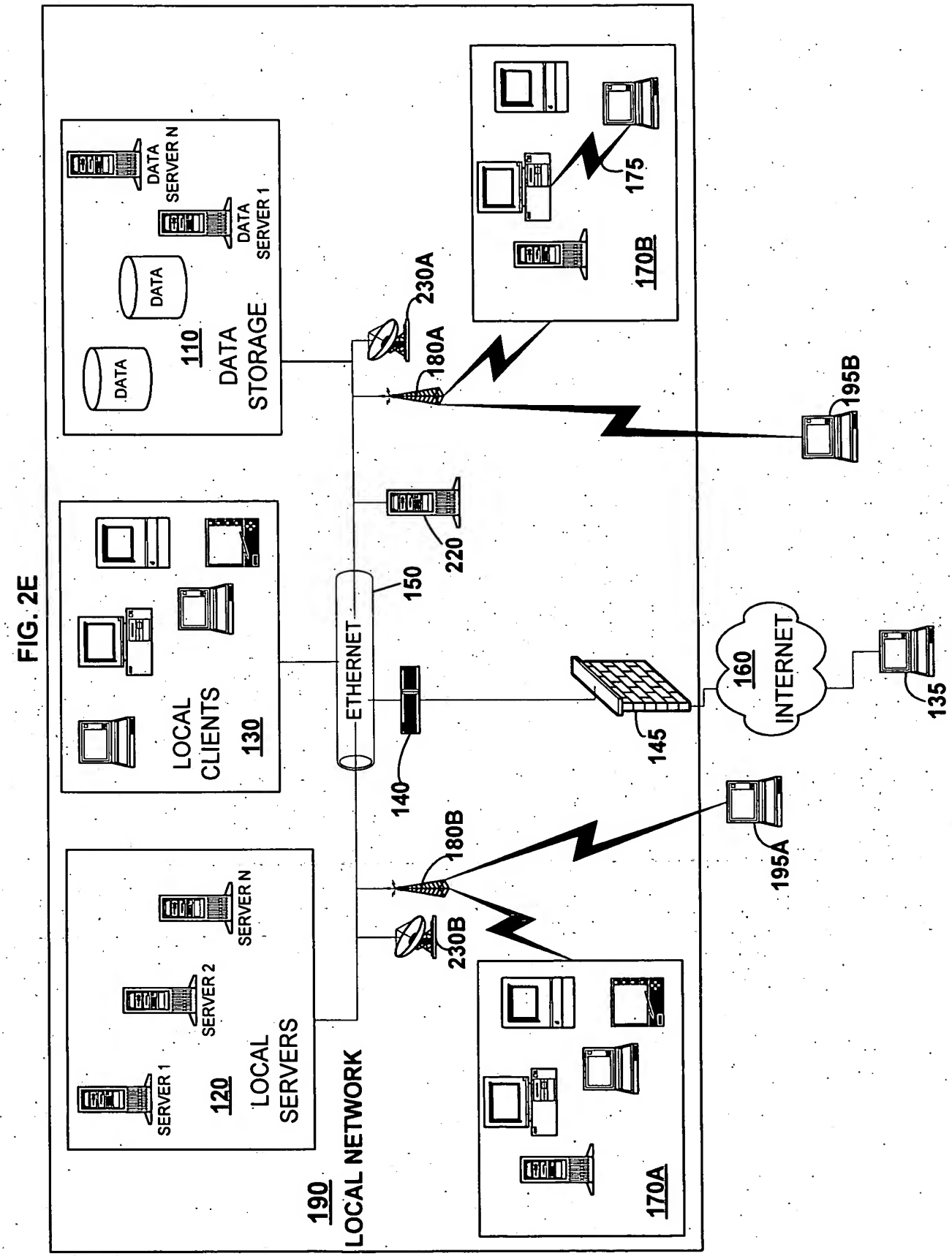

LOCAL NETWORK
190
DATA STORAGE
110
DATA
DATA
DATA SERVER N
DATA SERVER 1
LOCAL SERVERS
120
SERVER 1
SERVER 2
SERVER N
LOCAL CLIENTS
130
ETHERNET
150
140
145
160
INTERNET
135
170A
170B
175
180A
180B
195A
195B
220
230A
230B

FIG. 2E

FIG. 3

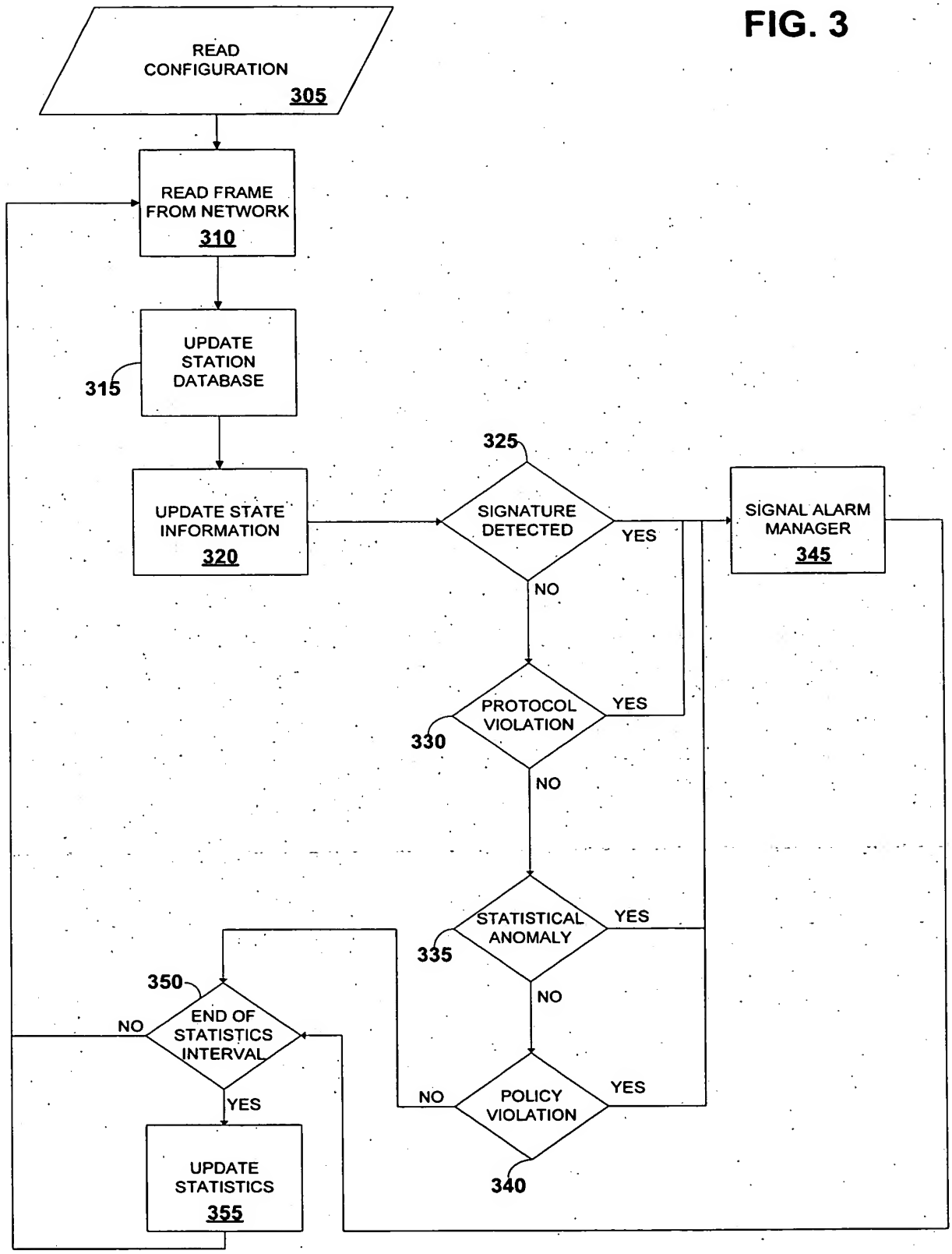

READ CONFIGURATION
305
READ FRAME FROM NETWORK
310
UPDATE STATION DATABASE
315
UPDATE STATE INFORMATION
320
325
SIGNATURE DETECTED
YES
NO
SIGNAL ALARM MANAGER
345
PROTOCOL VIOLATION
330
YES
NO
STATISTICAL ANOMALY
335
YES
NO
POLICY VIOLATION
340
YES
NO
350
END OF STATISTICS INTERVAL
YES
NO
UPDATE STATISTICS
355

FIG. 4

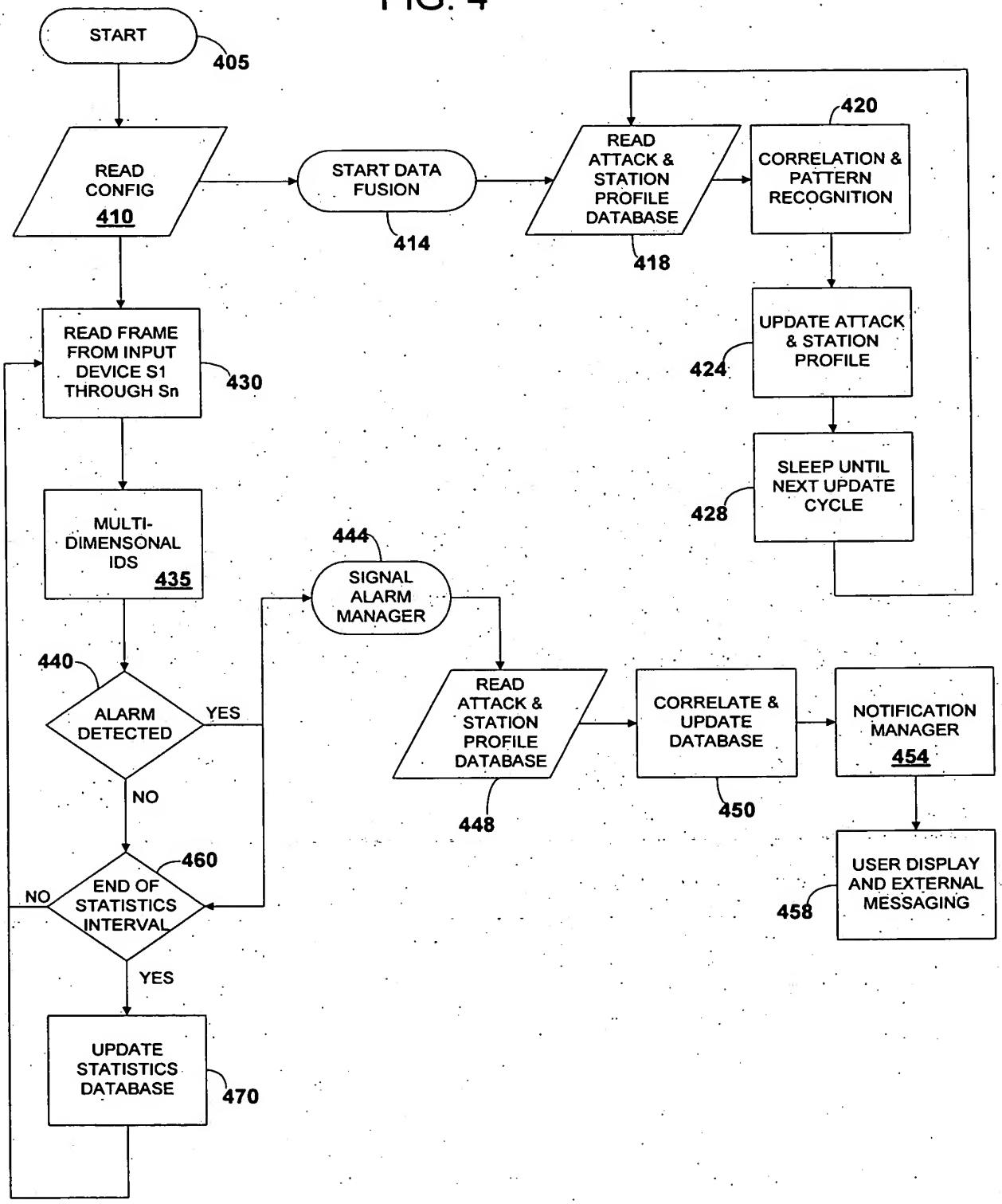

START
405
READ CONFIG
410
START DATA FUSION
414
READ ATTACK & STATION PROFILE DATABASE
418
420
CORRELATION & PATTERN RECOGNITION
UPDATE ATTACK & STATION PROFILE
424
SLEEP UNTIL NEXT UPDATE CYCLE
428
READ FRAME FROM INPUT DEVICE S1 THROUGH Sn
430
MULTI-DIMENSONAL IDS
435
444
SIGNAL ALARM MANAGER
440
ALARM DETECTED
YES
NO
READ ATTACK & STATION PROFILE DATABASE
448
CORRELATE & UPDATE DATABASE
450
NOTIFICATION MANAGER
454
USER DISPLAY AND EXTERNAL MESSAGING
458
460
END OF STATISTICS INTERVAL
NO
YES
UPDATE STATISTICS DATABASE
470

FIG. 5

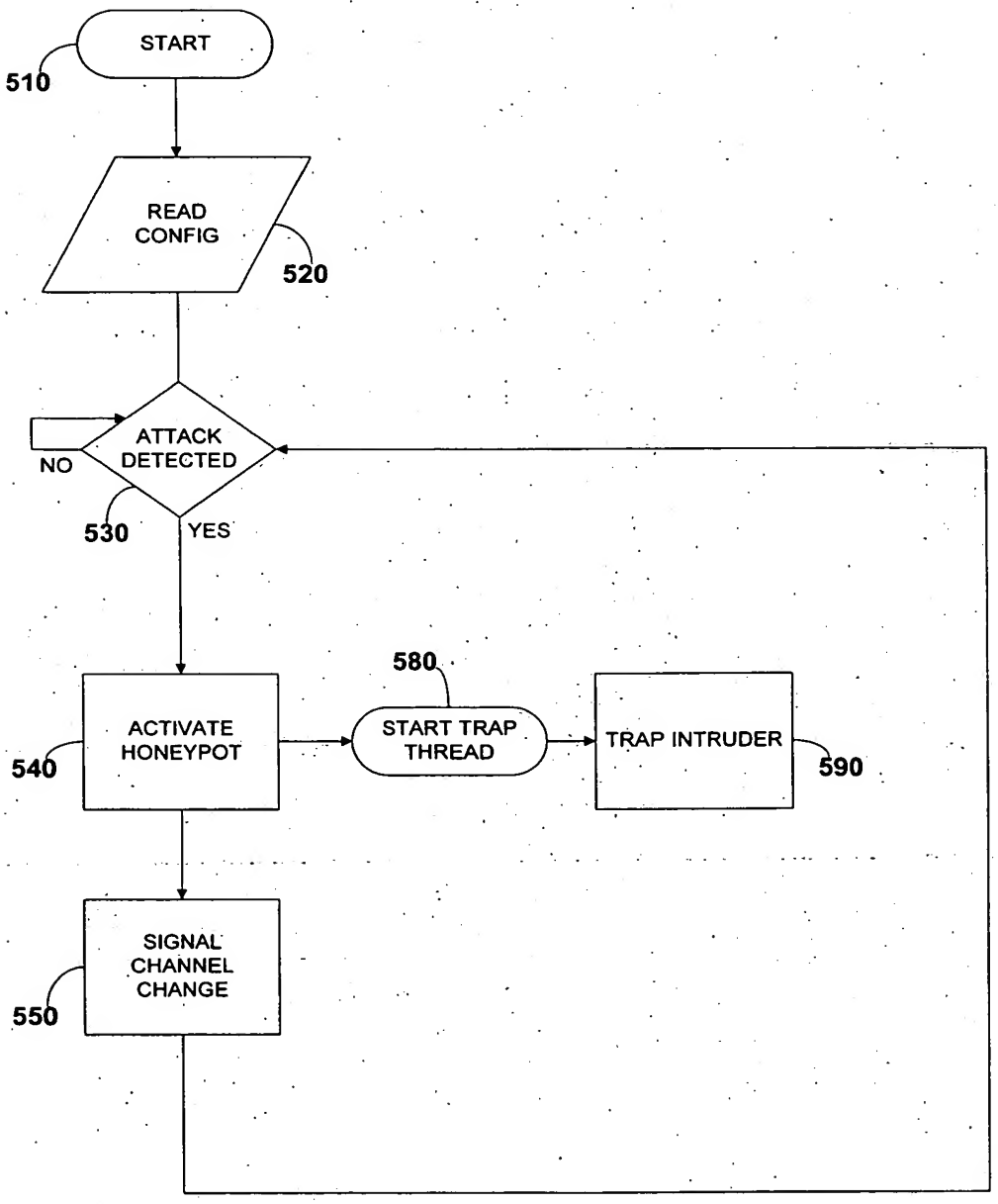

START
510
READ CONFIG
520
ATTACK DETECTED
NO
530
YES
580
ACTIVATE HONEYPOT
540
START TRAP THREAD
TRAP INTRUDER
590
SIGNAL CHANNEL CHANGE
550

FIG. 6A

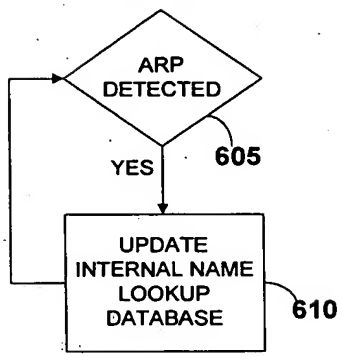

ARP DETECTED
605
YES
UPDATE INTERNAL NAME LOOKUP DATABASE
610

FIG. 6B

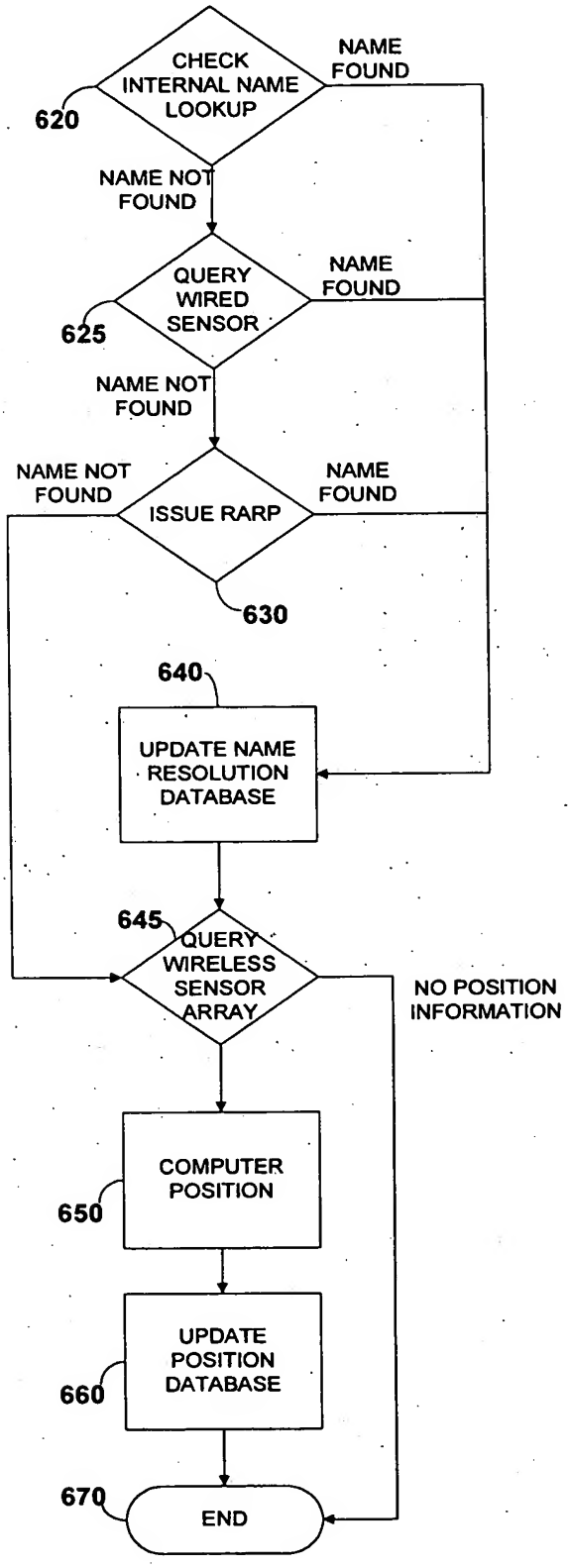

CHECK INTERNAL NAME LOOKUP
620
NAME FOUND
NAME NOT FOUND
QUERY WIRED SENSOR
625
NAME FOUND
NAME NOT FOUND
ISSUE RARP
NAME NOT FOUND
NAME FOUND
630
640
UPDATE NAME RESOLUTION DATABASE
645
QUERY WIRELESS SENSOR ARRAY
NO POSITION INFORMATION
COMPUTER POSITION
650
UPDATE POSITION DATABASE
660
670
END

FIG. 7A

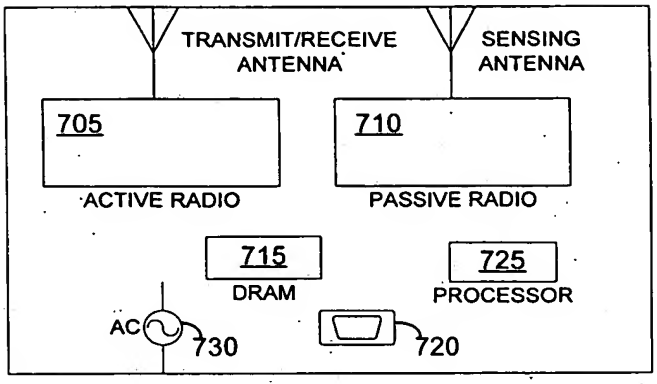


FIG. 7B

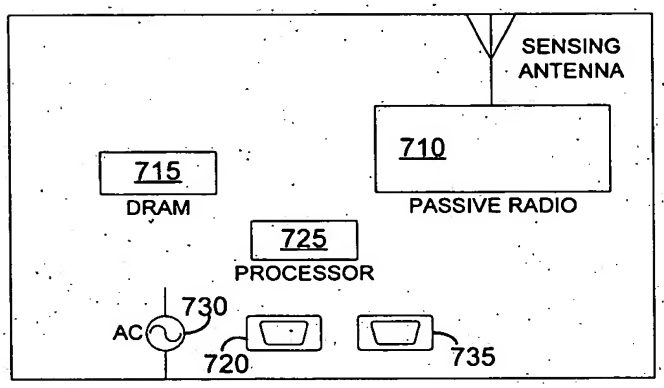


FIG. 7C

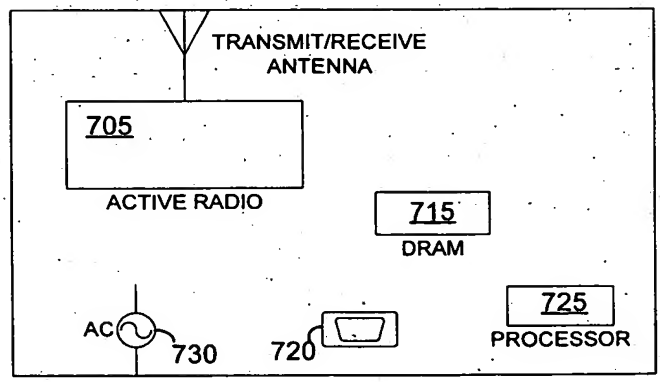


FIG 8A

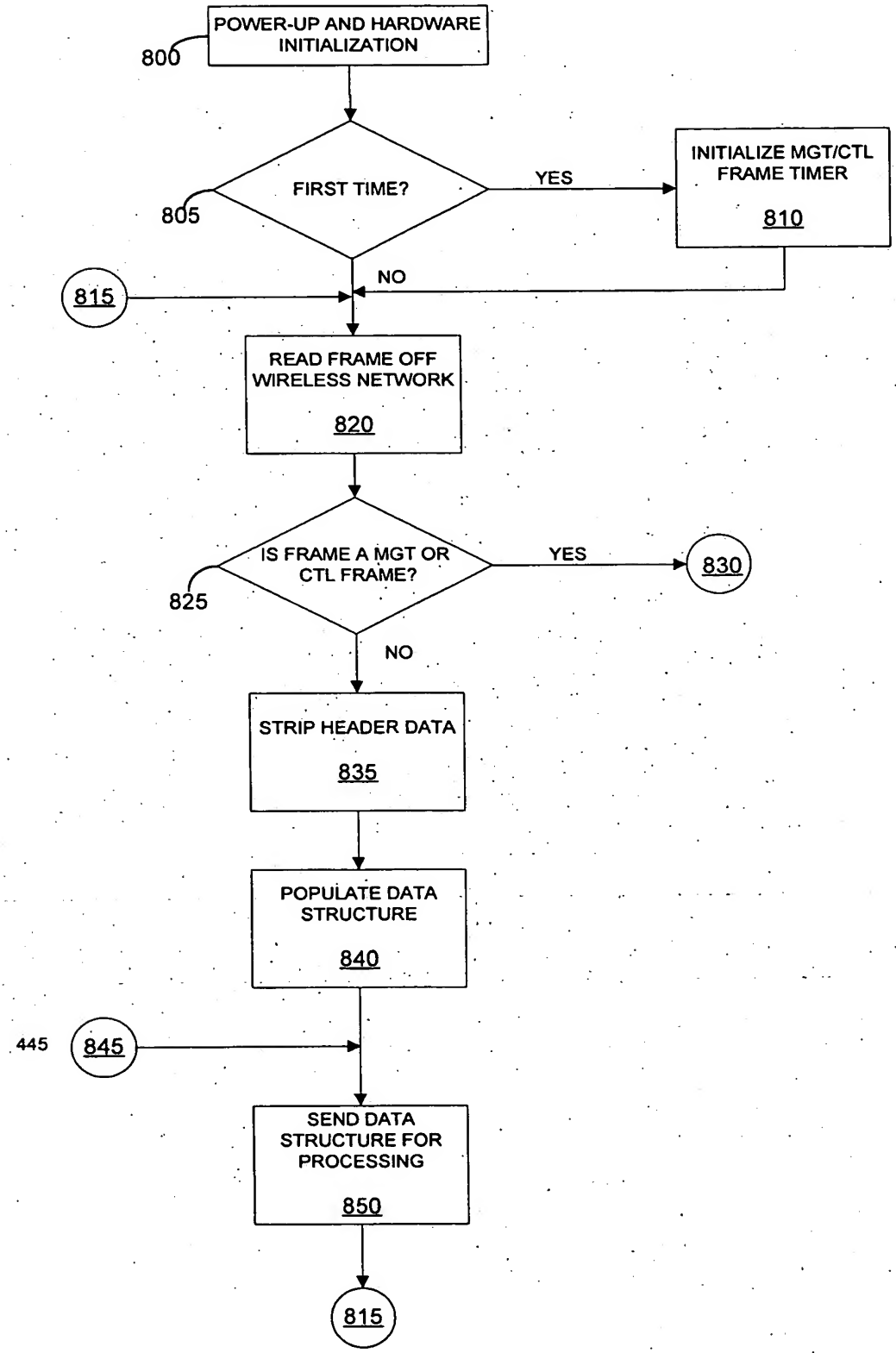

POWER-UP AND HARDWARE INITIALIZATION
800
FIRST TIME?
805
YES
INITIALIZE MGT/CTL FRAME TIMER
810
NO
815
READ FRAME OFF WIRELESS NETWORK
820
IS FRAME A MGT OR CTL FRAME?
825
YES
830
NO
STRIP HEADER DATA
835
POPULATE DATA STRUCTURE
840
445
845
SEND DATA STRUCTURE FOR PROCESSING
850
815

FIG 8B

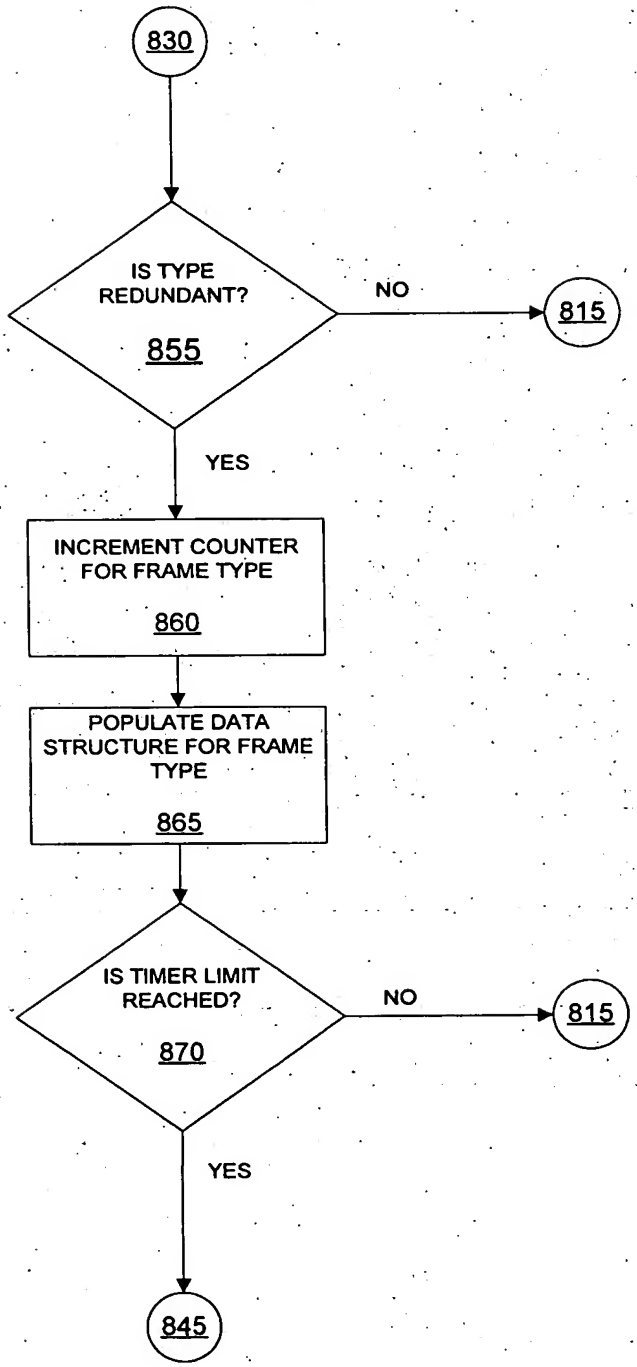

830
IS TYPE REDUNDANT?
855
NO
815
YES
INCREMENT COUNTER FOR FRAME TYPE
860
POPULATE DATA STRUCTURE FOR FRAME TYPE
865
IS TIMER LIMIT REACHED?
870
NO
815
YES
845

FIG. 9

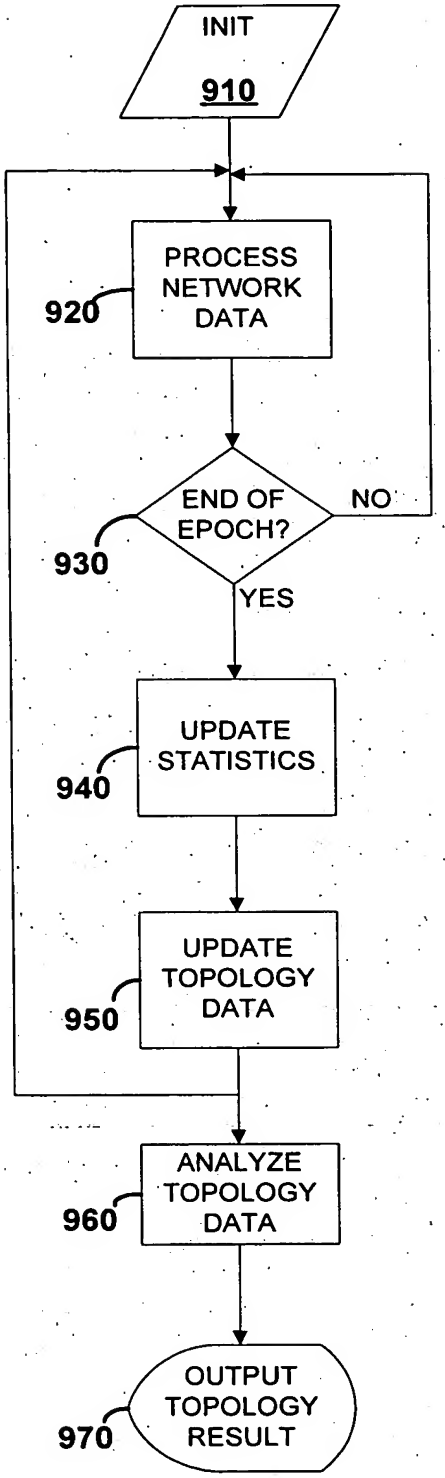

INIT
910
PROCESS NETWORK DATA
920
END OF EPOCH?
930
NO
YES
UPDATE STATISTICS
940
UPDATE TOPOLOGY DATA
950
ANALYZE TOPOLOGY DATA
960
OUTPUT TOPOLOGY RESULT
970

FIG. 10

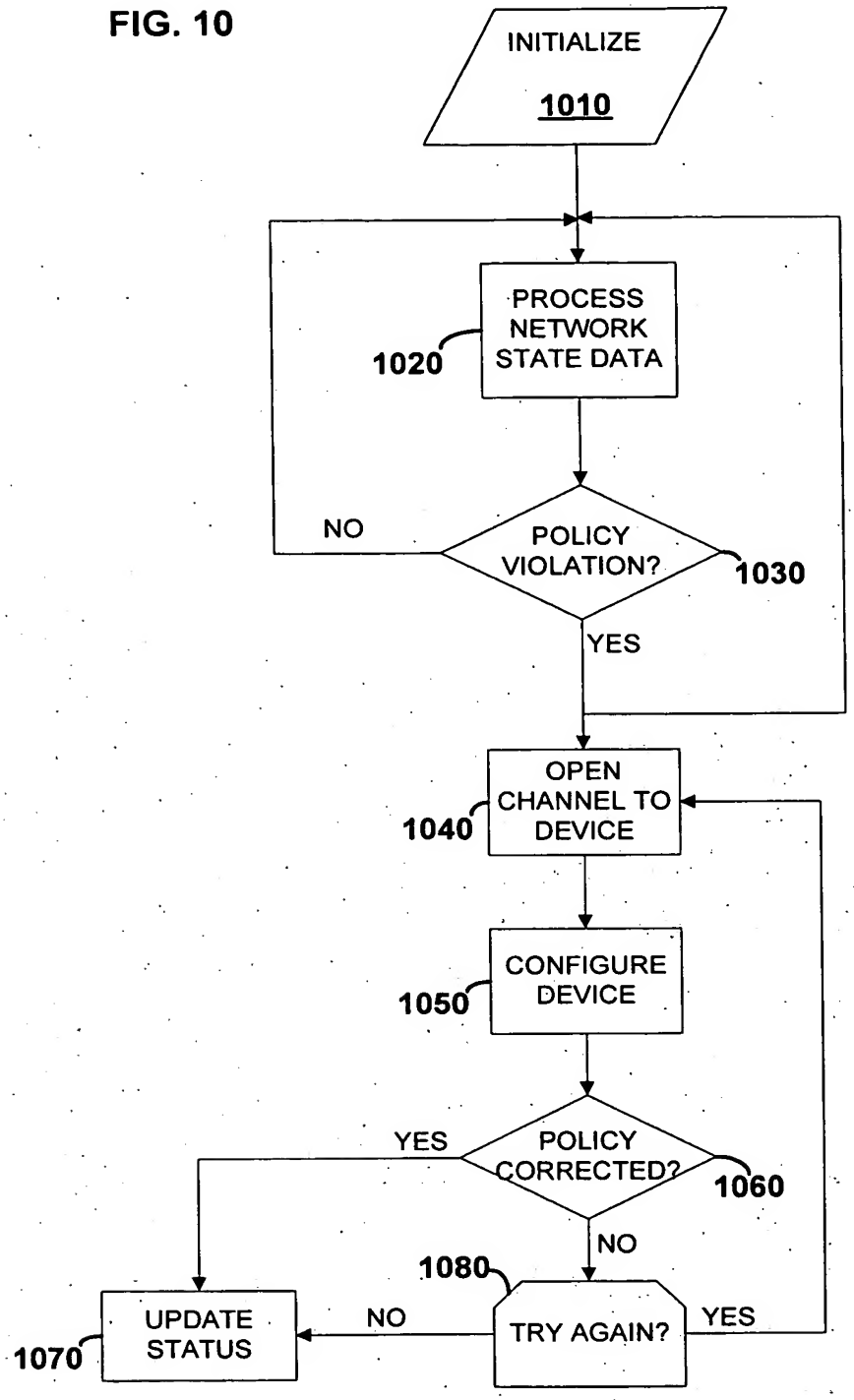
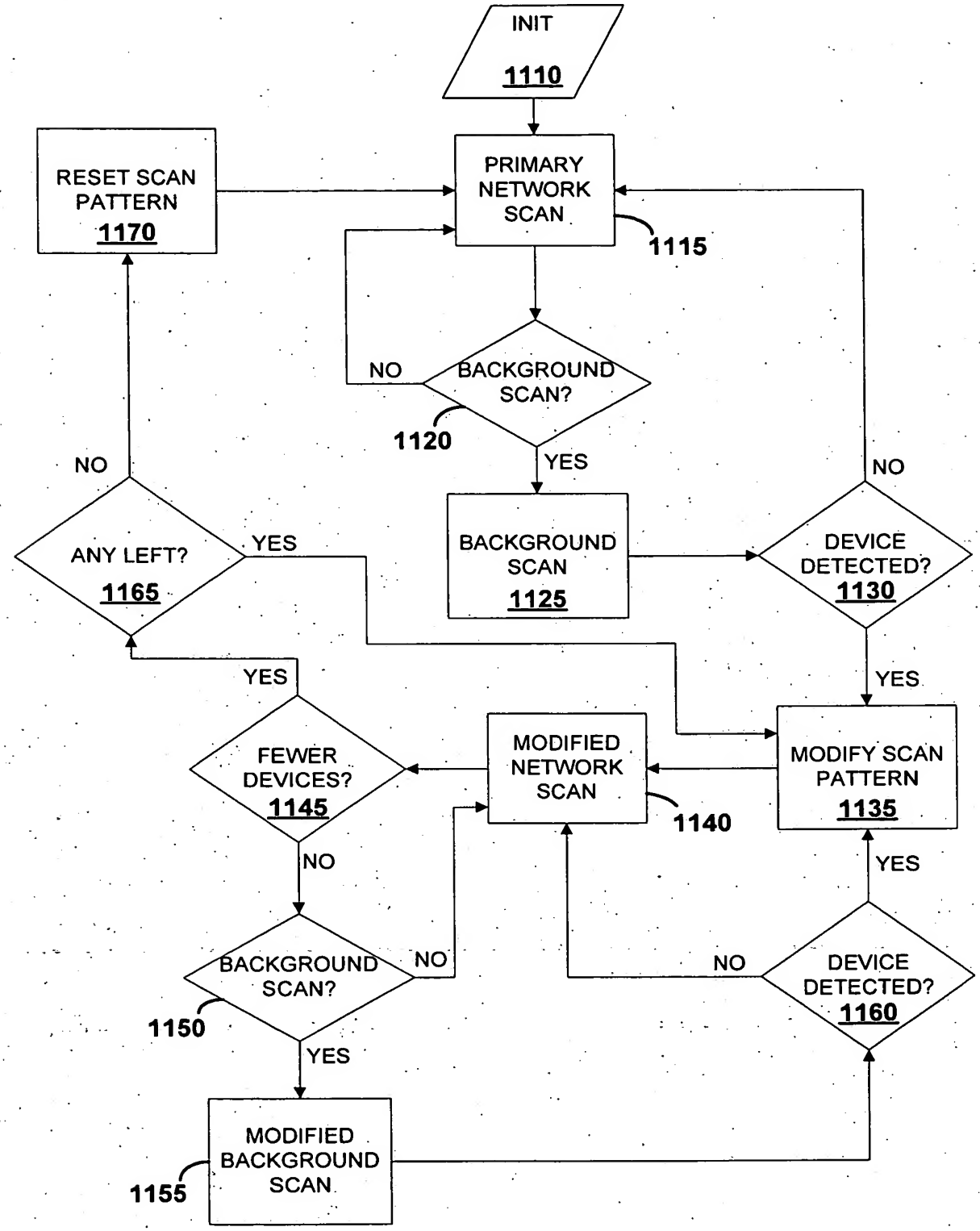

INITIALIZE
1010
PROCESS NETWORK STATE DATA
1020
POLICY VIOLATION?
1030
NO
YES
OPEN CHANNEL TO DEVICE
1040
CONFIGURE DEVICE
1050
POLICY CORRECTED?
1060
YES
NO
1080
TRY AGAIN?
NO
YES
UPDATE STATUS
1070

FIG. 11


INIT
1110
PRIMARY NETWORK SCAN
1115
RESET SCAN PATTERN
1170
NO
BACKGROUND SCAN?
1120
YES
NO
ANY LEFT?
1165
YES
BACKGROUND SCAN
1125
DEVICE DETECTED?
1130
NO
YES
YES
FEWER DEVICES?
1145
MODIFIED NETWORK SCAN
1140
MODIFY SCAN PATTERN
1135
NO
YES
BACKGROUND SCAN?
1150
NO
NO
DEVICE DETECTED?
1160
YES
MODIFIED BACKGROUND SCAN
1155

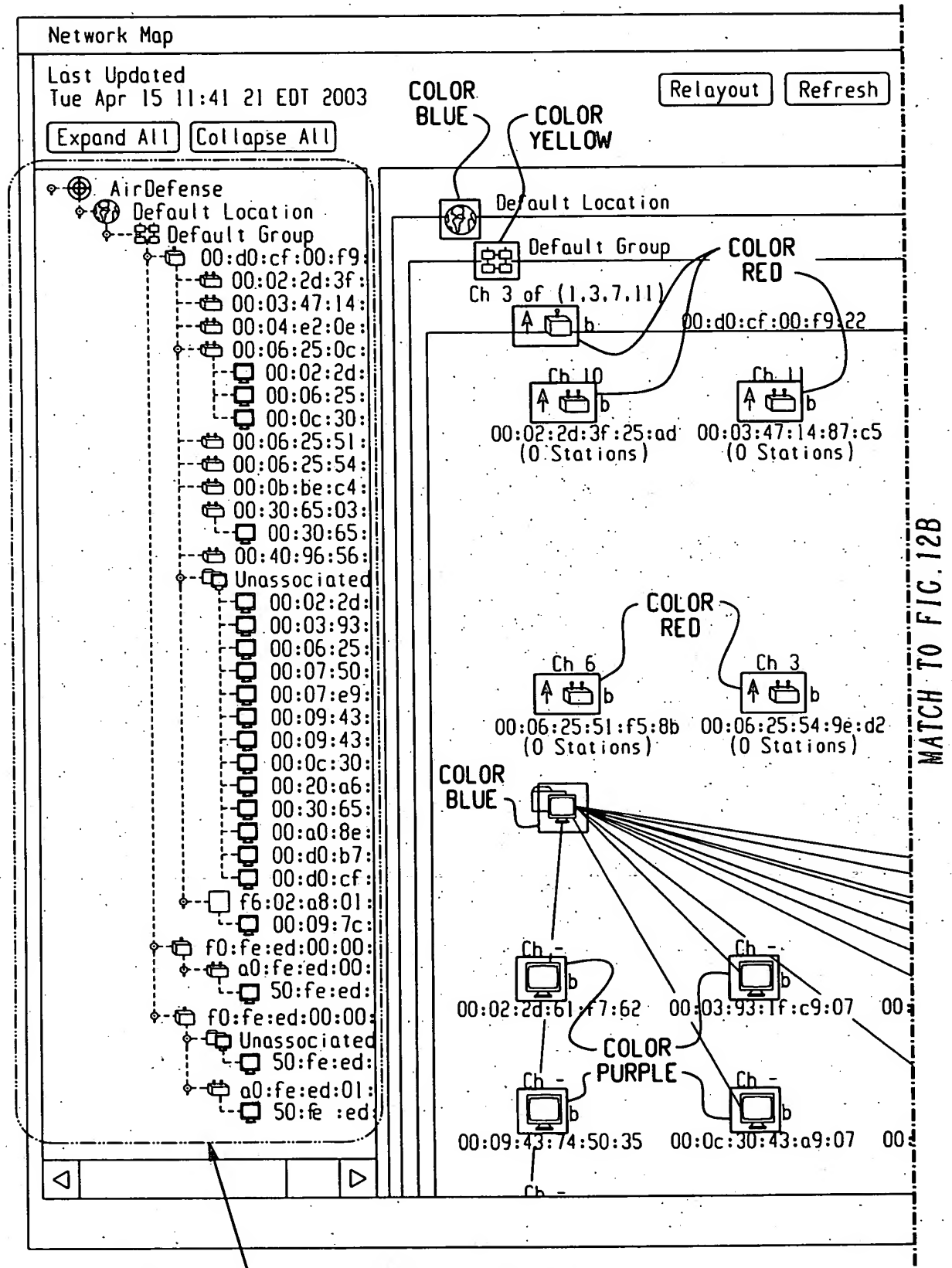


Fig. 12A1

Fig. 12A

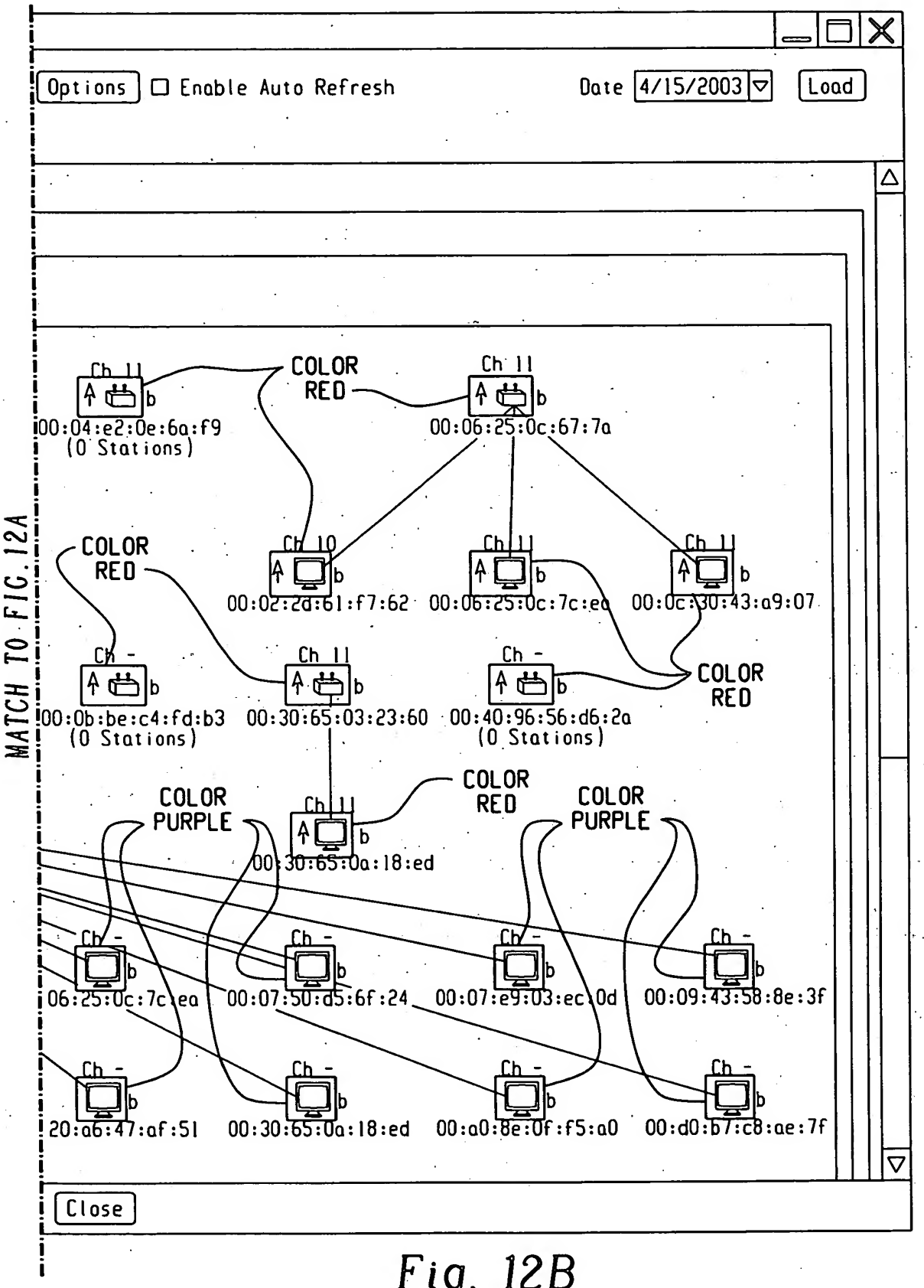

Options
Enable Auto Refresh
Date 4/15/2003
Load
MATCH TO FIG. 12A
Ch 11
00:04:e2:0e:6a:f9
(0 Stations)
COLOR RED
Ch 11
00:06:25:0c:67:7a
COLOR RED
Ch 10
00:02:2d:61:f7:62
Ch 11
00:06:25:0c:7c:ea
Ch 11
00:0c:30:43:a9:07
Ch -
00:0b:be:c4:fd:b3
(0 Stations)
Ch 11
00:30:65:03:23:60
Ch -
00:40:96:56:d6:2a
(0 Stations)
COLOR RED
COLOR PURPLE
Ch 11
00:30:65:0a:18:ed
COLOR RED
COLOR PURPLE
Ch -
06:25:0c:7c:ea
Ch -
00:07:50:d5:6f:24
Ch -
00:07:e9:03:ec:0d
Ch -
00:09:43:58:8e:3f
Ch -
20:a6:47:af:51
Ch -
00:30:65:0a:18:ed
Ch -
00:a0:8e:0f:f5:a0
Ch -
00:d0:b7:c8:ae:7f
Close

Fig. 12B

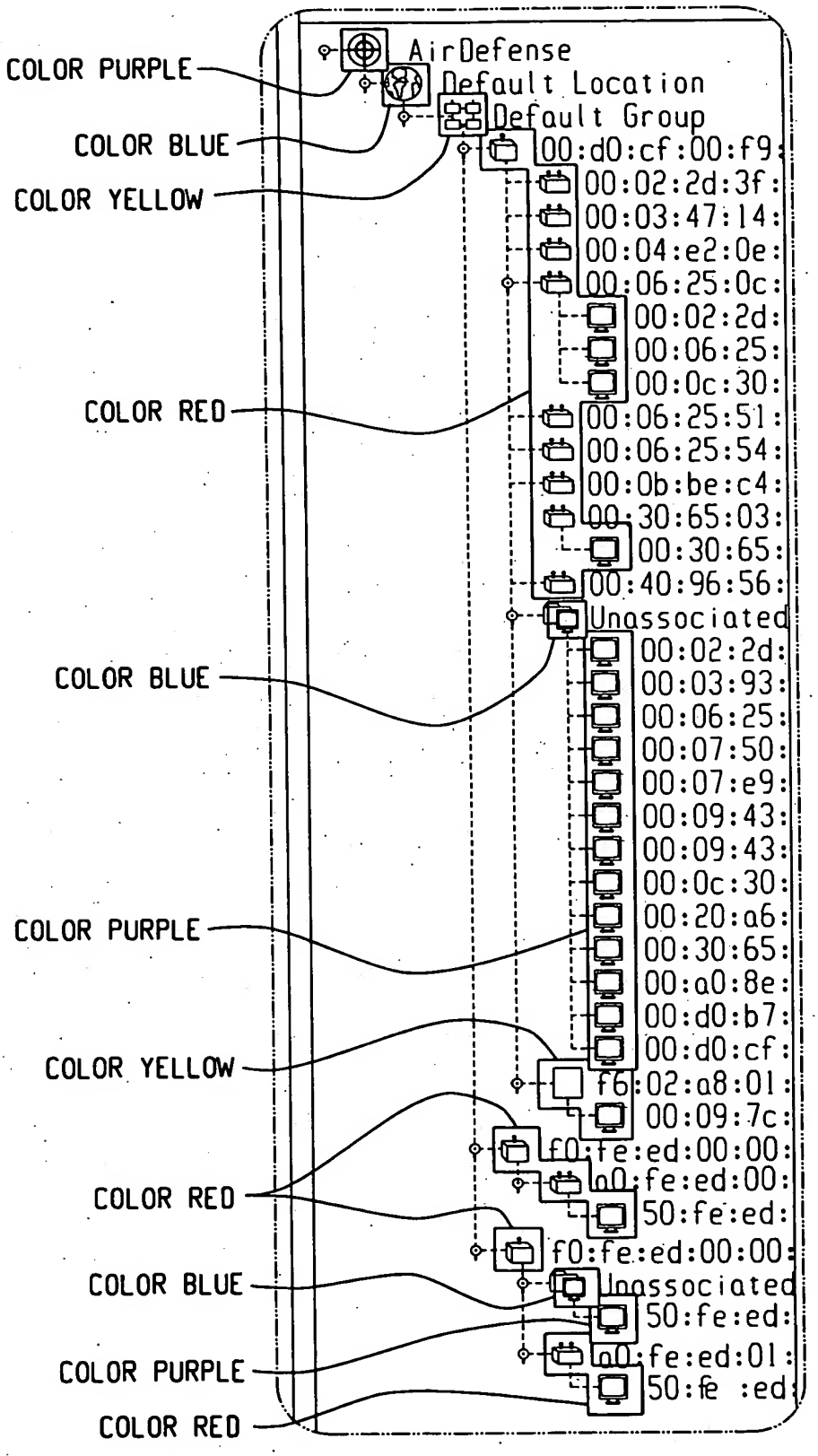

AirDefense
Default Location
Default Group
00:d0:cf:00:f9:
00:02:2d:3f:
00:03:47:14:
00:04:e2:0e:
00:06:25:0c:
00:02:2d:
00:06:25:
00:0c:30:
00:06:25:51:
00:06:25:54:
00:0b:be:c4:
00:30:65:03:
00:30:65:
00:40:96:56:
Unassociated
00:02:2d:
00:03:93:
00:06:25:
00:07:50:
00:07:e9:
00:09:43:
00:09:43:
00:0c:30:
00:20:a6:
00:30:65:
00:a0:8e:
00:d0:b7:
00:d0:cf:
f6:02:a8:01:
00:09:7c:
f0:fe:ed:00:00:
a0:fe:ed:00:
50:fe:ed:
f0:fe:ed:00:00:
Unassociated
50:fe:ed:
a0:fe:ed:01:
50:fe:ed:
COLOR PURPLE
COLOR BLUE
COLOR YELLOW
COLOR RED
COLOR BLUE
COLOR PURPLE
COLOR YELLOW
COLOR RED
COLOR BLUE
COLOR PURPLE
COLOR RED

Fig. 12A1

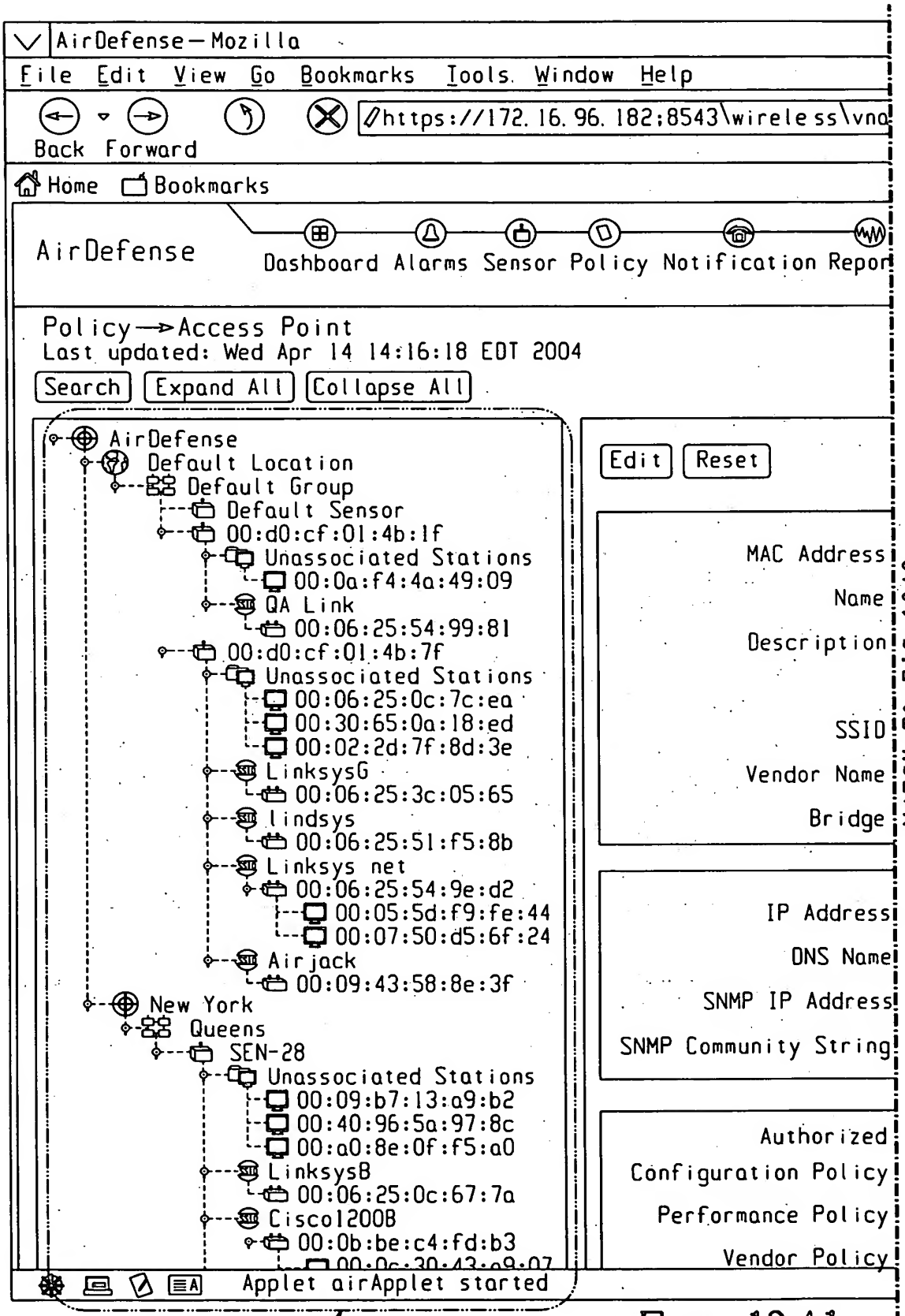


Fig. 13A1a

Fig. 13A1

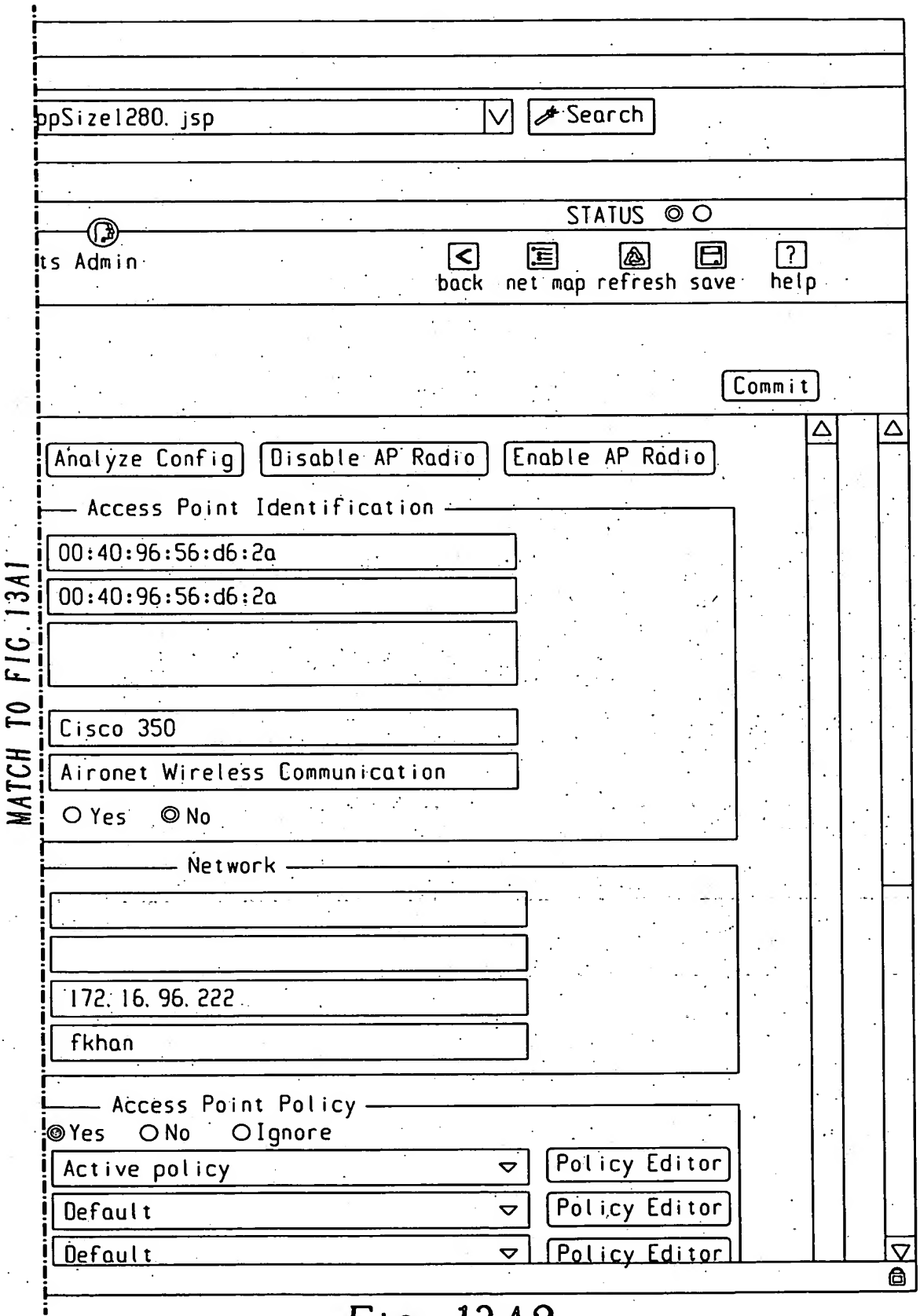

ppSize1280. jsp
Search
STATUS
ts Admin
back
net map
refresh
save
help
Commit
Analyze Config
Disable AP Radio
Enable AP Radio
Access Point Identification
00:40:96:56:d6:2a
00:40:96:56:d6:2a
Cisco 350
Aironet Wireless Communication
Yes
No
Network
172. 16. 96. 222
fkhan
Access Point Policy
Yes
No
Ignore
Active policy
Policy Editor
Default
Policy Editor
Default
Policy Editor
MATCH TO FIG. 13A1

Fig. 13A2

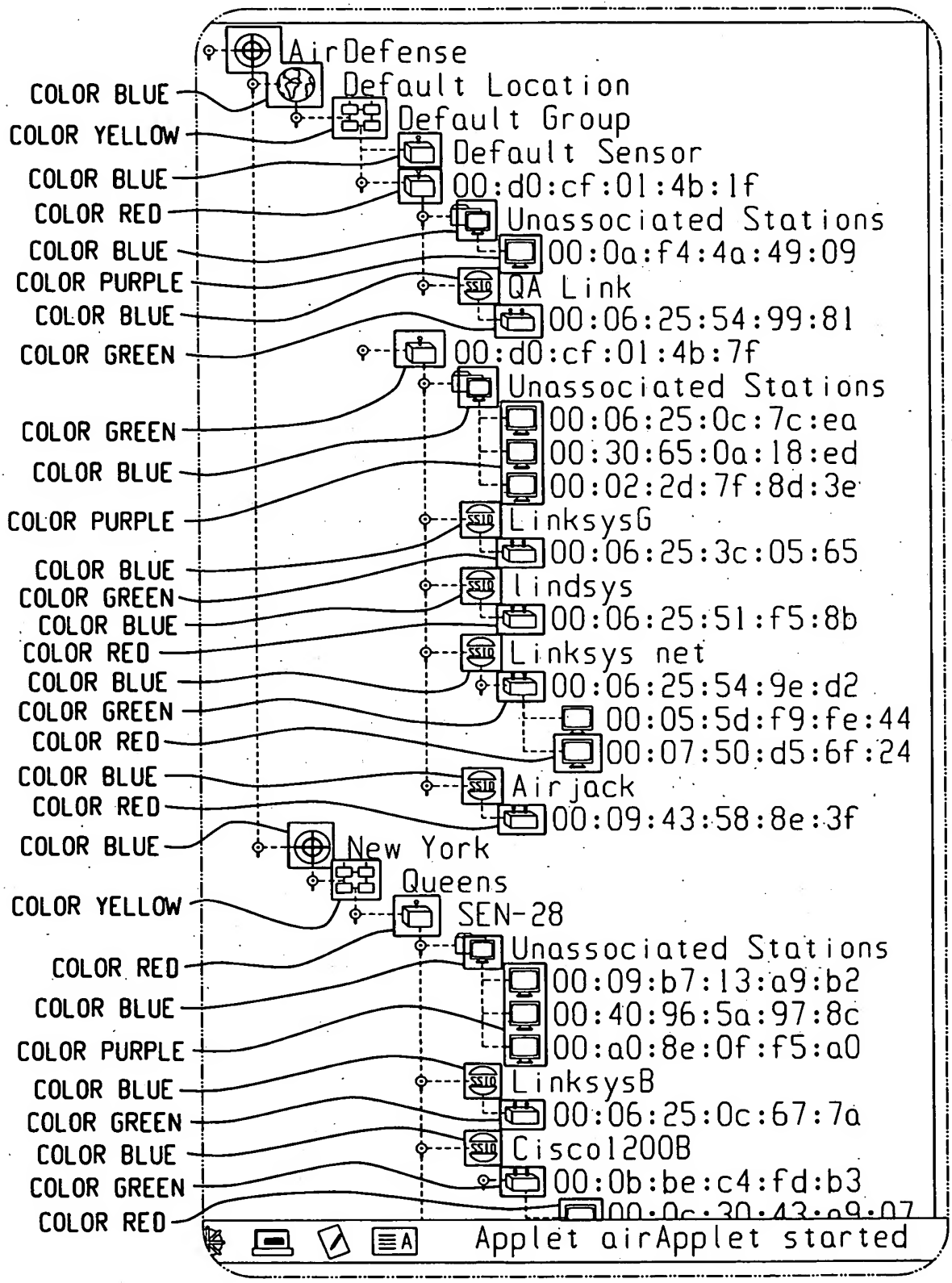

AirDefense
Default Location
Default Group
Default Sensor
00:d0:cf:01:4b:1f
Unassociated Stations
00:0a:f4:4a:49:09
QA Link
00:06:25:54:99:81
00:d0:cf:01:4b:7f
Unassociated Stations
00:06:25:0c:7c:ea
00:30:65:0a:18:ed
00:02:2d:7f:8d:3e
LinksysG
00:06:25:3c:05:65
lindsys
00:06:25:51:f5:8b
Linksys net
00:06:25:54:9e:d2
00:05:5d:f9:fe:44
00:07:50:d5:6f:24
Airjack
00:09:43:58:8e:3f
New York
Queens
SEN-28
Unassociated Stations
00:09:b7:13:a9:b2
00:40:96:5a:97:8c
00:a0:8e:0f:f5:a0
LinksysB
00:06:25:0c:67:7a
Cisco1200B
00:0b:be:c4:fd:b3
Applet airApplet started
COLOR BLUE
COLOR YELLOW
COLOR BLUE
COLOR RED
COLOR BLUE
COLOR PURPLE
COLOR BLUE
COLOR GREEN
COLOR GREEN
COLOR BLUE
COLOR PURPLE
COLOR BLUE
COLOR GREEN
COLOR BLUE
COLOR RED
COLOR BLUE
COLOR GREEN
COLOR RED
COLOR BLUE
COLOR RED
COLOR BLUE
COLOR YELLOW
COLOR RED
COLOR BLUE
COLOR PURPLE
COLOR BLUE
COLOR GREEN
COLOR BLUE
COLOR GREEN
COLOR RED

Fig. 13A1a

MATCH TO FIG. 13B2

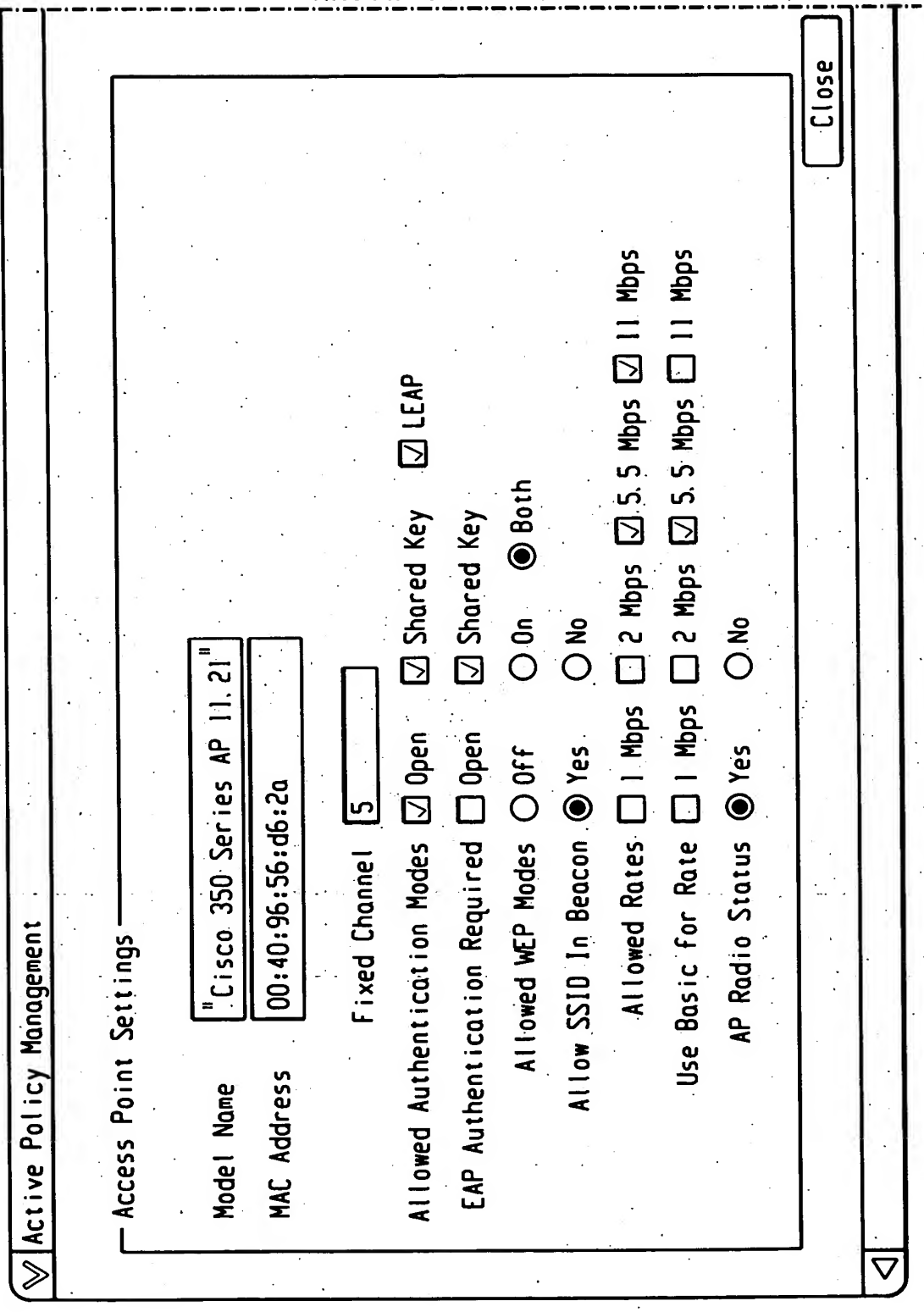


Fig. 13B1

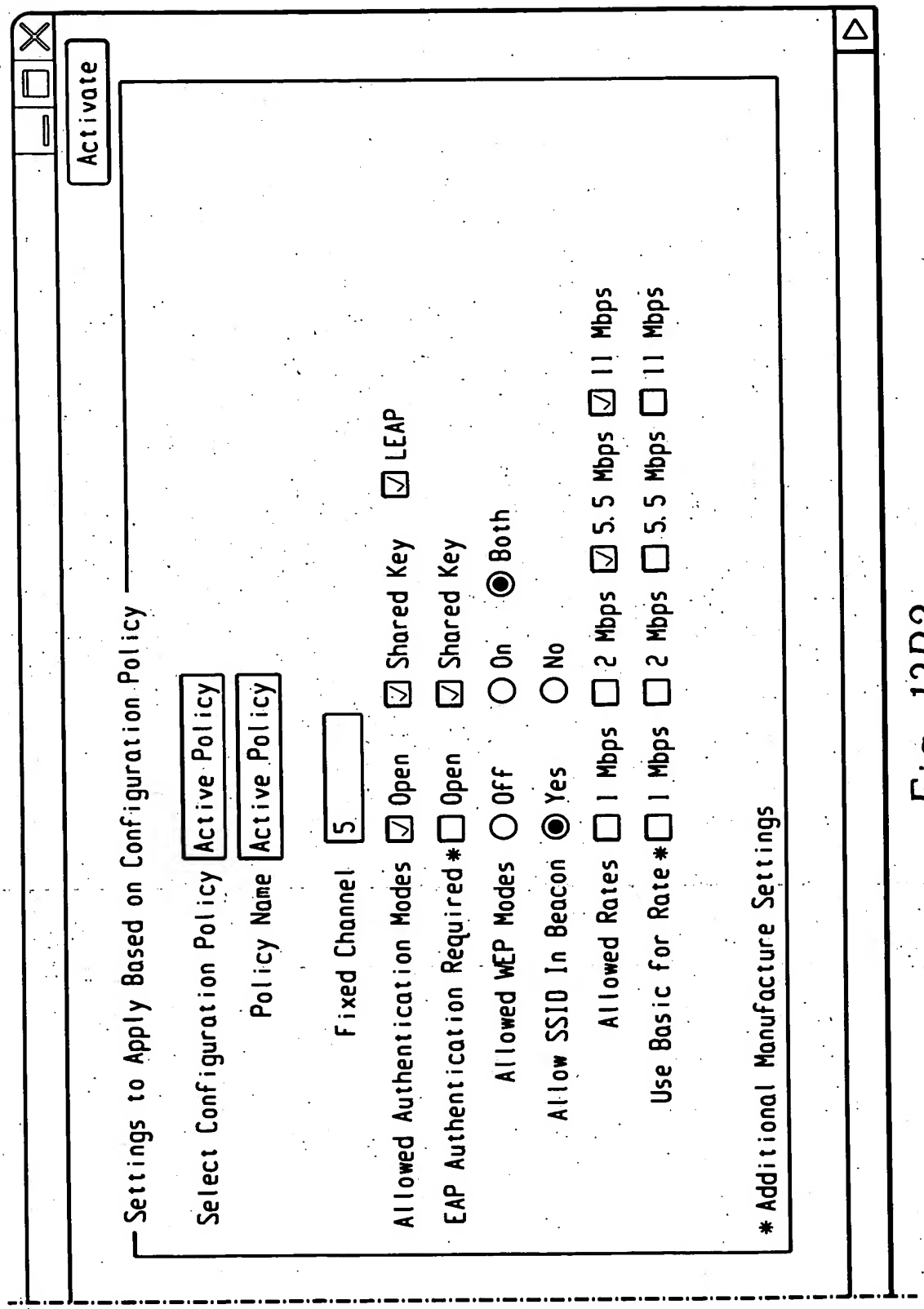


Fig. 13B2

MATCH TO FIG. 13B1

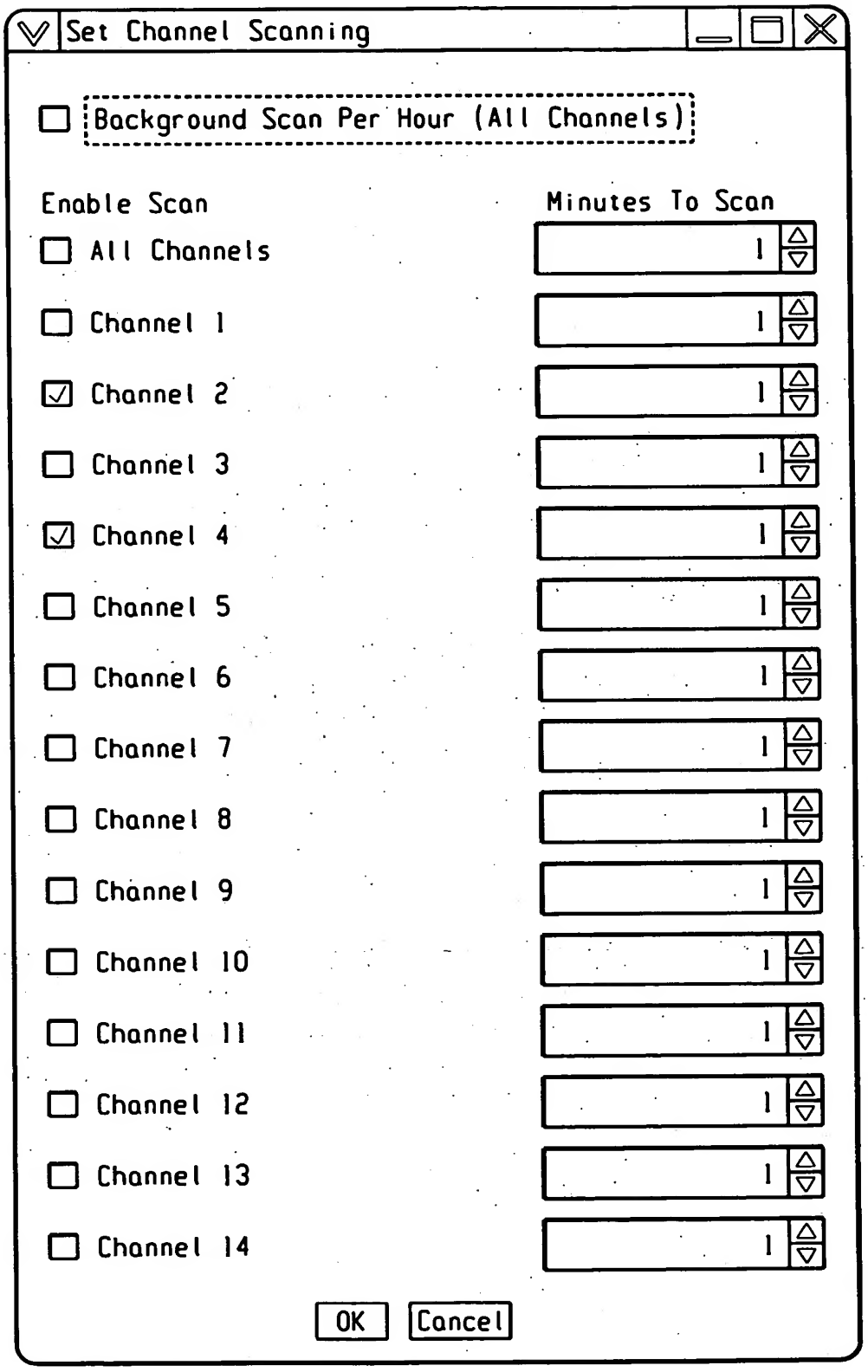

Set Channel Scanning
Background Scan Per Hour (All Channels)
Enable Scan
Minutes To Scan
All Channels
Channel 1
Channel 2
Channel 3
Channel 4
Channel 5
Channel 6
Channel 7
Channel 8
Channel 9
Channel 10
Channel 11
Channel 12
Channel 13
Channel 14
1
OK
Cancel

Fig. 14